IPSEC 優先ピア

IP セキュリティ（IPsec）優先ピア機能を使用すれば、フェールオーバー シナリオでクリプト マップ上の複数のピアが試行される環境を制御できます。

この機能には、次の機能が含まれます。

- デフォルト ピア設定
- デフォルト ピアでの IPsec アイドル タイマーの使用

- IPsec 優先ピアの前提条件 （1 ページ）
- IPsec 優先ピアの制約事項 （1 ページ）
- IPsec 優先ピアに関する情報 （2 ページ）
- IPsec 優先ピアの設定方法 （5 ページ）
- IPsec 優先ピアの設定例 （7 ページ）
- その他の参考資料 （7 ページ）
- IPsec 優先ピアの機能情報 （8 ページ）
- 用語集 （9 ページ）

IPsec 優先ピアの前提条件

- クリプト マップを正しく定義し、完成させておく必要があります。

IPsec 優先ピアの制約事項

デフォルト ピア

- この機能はデッド ピア検出（DPD）と組み合わせて使用する必要があります。定期モードで DPD が実行されている、リモート サイト上で使用するのが最も有効です。DPD によって、デバイスの障害が素早く検出され、デフォルト ピアが次に試行される接続用に試行されるようにピア リストがリセットされます。

- クリプト マップ内のデフォルト ピアとして指定できるピアは 1 つだけです。
- デフォルト ピアはピア リスト内の最初のピアである必要があります。

デフォルト ピアでの IPsec アイドル タイマーの使用

- この機能は、それが設定されているクリプトマップ上でだけ動作します。すべてのクリプト マップ用に機能をグローバルに設定はできません。
- グローバル アイドル タイマーが存在する場合、クリプトマップ アイドル タイマー値とグローバル値は異なっている必要があります。同じである場合、アイドルタイマーがクリプト マップに追加されません。

IPsec フェールオーバー

Cisco ASR 1000 シリーズ ルータの IPSec は、ステートレス フェールオーバーのみをサポートします。IPsec フェールオーバーは、IPsec ネットワークの合計稼働時間（または可用性）を増やす機能です。従来、これは元の（アクティブな）ルータに加えて冗長（スタンバイ）ルータを使用することで実現されています。アクティブ ルータが何らかの理由で使用できなくなると、スタンバイ ルータは、IKE および IPsec の処理を引き継ぎます。

IPsec フェールオーバーは、ステートスレス フェールオーバーおよびステートフル フェールオーバーの 2 種類に分類されます。ステートレス フェールオーバーは、ホット スタンバイ ルータ プロトコル（HSRP）のようなプロトコルを使用して、プライマリからセカンダリへのカットオーバーを行い、さらにアクティブおよびスタンバイの VPN ゲートウェイを許可して、共通の仮想 IP アドレスを共有することができます。

IPsec 優先ピアに関する情報

IPsec

IPsec は、インターネット技術特別調査委員会（IETF）によって開発されたオープン規格のフレームワークです。IPSec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。IPsecはネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（ピア）間のインターネット プロトコル（IP）パケットを保護および認証します。

IPSec は、次のネットワーク セキュリティ サービスを提供します。これらのサービスはオプションです。一般に、ローカル セキュリティ ポリシーにより、これらのサービスを 1 つ以上使用するよう指示されます。

- データ機密性：ネットワークにパケットを伝送する前に IPSec 送信側がパケットを暗号化できます。
- データ整合性：IPSec受信者は、IPSec送信者から送信されたパケットを認証し、伝送中にデータが変更されていないかを確認できます。

- データ送信元認証：IPSec受信者は、送信されたIPSecパケットの送信元を認証できます。
- アンチ リプレイ：IPsec 受信者は再送されたパケットを検出し、拒否できます。

IPSec を使用すれば、データを、観察、変更、またはスプーフィングされることを心配することなく、パブリック ネットワークを介して転送できます。これにより、インターネット、エクストラネット、およびリモート ユーザー アクセスを含む、バーチャル プライベート ネットワーク（VPN）などのアプリケーションが可能となります。

IPsec は、2 つのピア（2 台のルータなど）間にセキュア トンネルを確立します。機密性が高く、セキュア トンネルを介して送信する必要があるパケットを定義し、セキュア トンネルの特性を指定することによって、機密性の高いパケットを保護するパラメータを定義します。IPsec ピアによってこのように機密性の高いパケットが検出されたら、そのピアによって、適切な、セキュアなトンネルが設定され、そのパケットがトンネルからリモート ピアに送信されます。

Dead Peer Detection

VPN クライアントでは、DPD と呼ばれるキープアライブ メカニズムが使用され、IPsec トンネルの反対側の VPN デバイスが利用できるかどうかがチェックされます。ネットワークが極端にビジーだったり、信頼性が低下していたりした場合、ピアがこれからアクティブになることがないかどうか判断するまで VPN クライアントが待機する時間の秒数を増加できます。

トラフィックが受信されると、キープアライブ パケットは送信されません。これにより、DPD に関連したオーバーヘッドが低下します。高い負荷がかかっているネットワーク上では、トラフィックがトンネル上で受信されるために、送信されるキープアライブ パケットがきわめて少なくなるからです。さらに、DPD によってキープアライブ パケットが送信されるのは、送信されるユーザ トラフィックがある（そして受信されるユーザ トラフィックがない）場合だけです。

インターネット キー交換（IKE）を、発信ユーザ データが存在しているかどうかにかかわらず DPD によってキープアライブ パケットが送信されるように設定できます。つまり、受信ユーザ データがないかぎり、キープアライブパケットは設定されたキープアライブ インターバルで送信されます。

デフォルト ピア設定

接続タイムアウトが発生した場合、現在のピアへの接続は終了します。**set peer** コマンドを使用すれば、最初のピアをデフォルトピアとして設定できます。デフォルトピアが存在している状態で次回の接続が開始された場合、その接続は、ピア リスト内の次のピアではなく、デフォルト ピアに直接接続されます。デフォルト ピアの応答がない場合、ピア リスト内の次のピアが現在のピアとなり、クリプトマップを介した次からの接続では、そのピアが試行されます。

この機能は、物理リンク上のトラフィックがリモートピアの障害により停止した場合に便利です。DPD によって、リモート ピアが使用できないことが示されますが、そのピアは現在のピアのままです。

デフォルト ピアによって、過去に使用不可になったがサービスに復帰した優先ピアへのフェールオーバーが容易になります。ユーザは、特定のピアに対してフェールオーバーのイベントにおけるプリファレンスを与えることが可能です。これは、元の障害の原因がリモート ピアの障害ではなく、ネットワーク接続の問題であった場合に便利です。

アイドル タイマー

ルータでピアの IPSec セキュリティ アソシエーション（SA）を作成する場合、SA を維持するためのリソースを割り当てる必要があります。SA には、メモリと、複数の管理されたタイマーが必要です。ピアがアイドル状態だと、それらのリソースが無駄になってしまいます。あまりに多くのリソースがアイドル状態のピアによって浪費されてしまうと、ルータによる他のピアとの新しい SA の作成ができなくなる可能性があります。

IPsec SA アイドル タイマーを使用すると、アイドル状態のピアに関連した SA を削除することによってリソースの可用性を高めることが可能です。IPsec SA アイドル タイマーによってアイドル状態のピアによるリソースの浪費が防止されるので、必要に応じて新しい SA を作成するためにより多くのリソースを利用できるようになります。

IPsec SA アイドル タイマーが設定されていない場合、IPsec SA のグローバル ライフタイムだけが適用されます。SA は、ピアのアクティビティと関わりなく、グローバル タイマーが有効期限切れになるまで維持されます。

デフォルト ピアでの IPsec アイドル タイマーの使用

現在のピアへのすべての接続がタイムアウトした場合、次に接続が開始された時には、**set peer** コマンドで設定されたデフォルト ピアに直接接続されます。デフォルト ピアが設定されていない状態で接続タイムアウトが発生した場合、現在のピアはタイムアウトしたピアのままになります。

この機能拡張により、過去に使用不可になったが現在では稼働中の優先ピアに対するフェールオーバーが容易になります。

クリプト マップ上のピア

クリプト マップ セットには複数のエントリを含めることができ、それぞれが異なるアクセス リストに対応します。ルータでは、クリプト マップ エントリが順番に検索され、そのエントリ内で指定されたアクセス リストとパケットの照合が試行されます。

パケットが特定のアクセスリスト内の **permit** エントリと一致し、対応するクリプトマップエントリが Cisco としてタグが付けられていた場合、クリプトマップ内のピア設定ステートメントで指定されたリモートピアとの接続が確立されます。

IPsec 優先ピアの設定方法

デフォルト ピアの設定

デフォルト ピアを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]
4. **set peer** {*host-name* [**dynamic**] [**default**] | *ip-address* [**default**] }
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*] 例： `Router(config)# crypto map mymap 10 ipsec-isakmp`	クリプト マップ コンフィギュレーション モードを開始します。クリプト マップ エントリを作成または変更するか、動的に作成されるクリプトマップ設定のテンプレートを提供する暗号プロファイルを作成するか、またはクライアント アカウンティング リストを設定します。
ステップ 4	**set peer** {*host-name* [**dynamic**] [**default**]	*ip-address* [**default**] } 例： `Router(config-crypto-map)# set peer 10.0.0.2 default`	クリプト マップ内の IPsec ピアを指定します。指定した最初のピアがデフォルト ピアとして定義されていることを確認します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config-crypto-map)# exit`	クリプト マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

アイドル タイマーの設定

アイドル タイマーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]
4. **set security-association idletime** *seconds* [**default**]
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*] 例： `Router(config)# crypto map mymap 10 ipsec-isakmp`	クリプト マップ コンフィギュレーション モードを開始します。クリプト マップ エントリを作成または変更するか、動的に作成されるクリプトマップ設定のテンプレートを提供する暗号プロファイルを作成するか、またはクライアント アカウンティング リストを設定します。
ステップ 4	**set security-association idletime** *seconds* [**default**] 例： `Router(config-crypto-map)# set security-association idletime 120 default`	デフォルト ピアが使用される前に、現在のピアをアイドル状態にしておける最大期間を指定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config-crypto-map)# exit`	クリプト マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

IPsec 優先ピアの設定例

デフォルト ピアの設定例

次に、IP アドレスが 10.1.1.1 である最初のピアがデフォルト ピアである例を示します。

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
```

IPsec アイドル タイマーの設定例

次の例では、現在のピアが 120 秒間アイドルであった場合、次の接続試行ではデフォルトピア 10.1.1.1（**set peer** コマンドで指定）が使用されます。

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
 set security-association idletime 120 default
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPSec	『*Security for VPNs with IPsec*』
クリプト マップ	• 『*Security for VPNs with IPsec*』 • 「*Configuring Internet Key Exchange for IPsec VPNs*」
DPD	『*IPsec Dead Peer Detection Periodic Message Option*』

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPsec 優先ピアの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : IPsec* 優先ピアの機能情報

機能名	リリース	機能情報
IPSEC 優先ピア	Cisco IOS XE Release 2.1	IPsec 優先ピア機能を使用すれば、フェールオーバー シナリオでクリプト マップ上の複数のピアが試行される環境を制御できます。 次のコマンドが導入または変更されました。**set peer** (IPsec) および **set security-association idle-time**。

用語集

crypto access list：暗号によって保護する IP トラフィック、および暗号によって保護しないトラフィックが定義されたリスト。

crypto map：IPsec によって保護する必要があるトラフィック、送信する必要がある IPsec 保護対象トラフィック、およびこのトラフィックに適用する必要がある IPsec トランスフォームセットが指定されたマップ。

dead peer detection：応答しないピアを検出することをルータに可能にさせる機能。

keepalive message：1 つのネットワークデバイスからもう 1 つのネットワークデバイスに対して、2 つのネットワークデバイス間の仮想回線がまだアクティブであることを通知するために送信されるメッセージ。

peer：IPsec および IKE に参加するルータまたはその他のデバイス。IPsec においては、ピアは、キーの交換またはデジタル証明書の交換のどちらかを通じてセキュアに通信するデバイスまたはエンティティです。

SA：Security Association（セキュリティ アソシエーション）。データ フローに適用されるセキュリティ ポリシーとキー関連情報のインスタンスです。SA は、IKE と IPsec の双方で使用されますが、各 SA は互いに独立しています。IPsec SA は単方向通信であり、セキュリティ プロトコルごとに一意です。IKE SA は、IPsec SA とは異なって双方向通信であり、使用されるのは IKE に限られます。SA のネゴシエーションおよび確立は、IPsec ではなく IKE によって行われます。また、IPsec SA はユーザが手動で確立できます。保護されたデータ パイプでは 1 組の SA が必要であり、プロトコルごとに 1 方向あたり 1 つずつ必要です。たとえば、ピア間でカプセル化セキュリティ ペイロード（ESP）をサポートするパイプに対しては、それぞれの通信方向ごとに 1 つの ESP SA が必要です。SA は、宛先（IPsec エンドポイント）のアドレス、セキュリティ プロトコル（AH または ESP）、およびセキュリティ パラメータ インデックス（SPI）によって一意に識別されます。

transform set：IPsec 保護されたトラフィックに適用されるセキュリティプロトコル、アルゴリズムおよびその他の設定の適切な組み合わせです。IPsec SA のネゴシエーション中に、ピアは、特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。